ABSTRACT

A method of producing a system architecture comprises identifying a set of undesirable events and ascribing to each of the undesirable events an indicator of their severity, associating the undesirable events with one or more actuators of the system architecture, developing a functional specification of an initial architecture proposed for implementation of the system architecture, refining fault tolerance requirements associated with the severity of each of the undesirable events and issuing refined fault tolerance requirements, producing replicates in the functional specification together with attached indicators of freeness of the replicates from other of the replicates, the indicators reflecting the refined fault tolerance requirements, defining a hardware structure for the system architecture, mapping the functional specification onto the hardware structure, and verifying automatically that the indicators of freeness are preserved during the mapping. The method can be stored on a computer readable storage medium or implemented by a design tool.